HOPE CHRISTIAN COLLEGE
A Ministry of Craigmore Christian Church

POLICY PAPER

Computer & Communication Device Use

Policy No. IT707

Rationale

At Hope Christian College (College), we understand that Information Communication Technology (ICT) is part of everyday life. In the term ICT we include all computers (portable or desktop) and other devices that allow communication via online or electronic means or access to the internet, including but not limited to, smartphones, tablets, smartwatches, laptops, gaming devices, electronic recording devices, or any device with blue-tooth capability or containing a SIM card.

The College does not allow a student's own device to be used onsite. However, when using College ICT devices, the same standards of communication and interaction apply to ICTs as they do to face-to-face communications. The College ICTs are to assist in learning knowledge and skills, not for personal use.

Aim

This policy is an overarching guide for the College community on how ICTs should be used in the College environment. Parents and students should also see the most current edition of the *Student Portable Device Program Handbook* for more details especially concerning senior school students.

Policy statement

The policy of the College is two-fold:

- student's use of College ICTs must be strictly in line with the conditions outlined in this policy and with signed student agreements, and must be used safely and for educational purposes only
- use of personal ICT devices, including mobile phones and smartwatches is not to occur while a student is at College or involved in College activities.

Scope

This policy is to guide College students and parents concerning acceptable behaviour and use of their own or College ICTs.

Definitions

at/to the College – this refers to being on the College grounds, but also refers to being present at College activities such as excursions, on or off site, and special days (e.g. Sports Days) and requires adherance to this policy unless specified by a separate policy or when specific permission is given by the responsible staff member

College community – this includes but may not be limited to: students, parents of students, immediate family of students, authorised volunteers, authorised visiting speakers and guests, staff (whether temporary, contracted or permanent), staff spouses and dependent children (who are not staff or family), College leadership, OSHC and CCC staff and leadership who are connected in some way to the College (e.g. not unconnected church attendees)

parent – includes caregivers and guardians, or the responsible person as listed on the enrolment form

social media – refers to online communities sharing comments and content, via web or apps

staff – refers to the student's class teacher or a paid Hope Christian College staff member who is responsible for supervising the student during College hours or activities

student – any student enrolled at Hope Christian College through a contract with their parent/guardian(s), regardless of their age

1. Overarching conditions for all College ICT use

All students must use College issued devices ensuring that all students have resources of equal quality, and the ability to access IT support when there is a fault or problem. Students cannot use their own devices at College. Furthermore:

- Students may have no expectation of privacy with College computers including e-mail and stored files.
- The College retains control, custody, and supervision of all computers, networks, and Internet services owned or leased by the College, except where a graduating Year 12 student opts to make a 'balloon' payment which transfers ownership of the portable device to them upon their departure.
- The College reserves the right to monitor all computer and Internet activity by students using College equipment, network or account.
- Students and/or parents shall be responsible for compensating the College for any costs due to loss or damage related to vandalism, failure to follow HCC rules or deliberate misuse of ICTs and their consumables (e.g. power packs, cords, carry bags).
- No member of the College community may use any College ICT for any illicit or illegal activities and may not use methods such as proxy servers to bypass the College network security, whether on site or elsewhere. Illegal use will be referred to the Police.
- In the event of loss or theft of College ICT, a Police Report and Incident Number must be obtained, and the loss reported to the appropriate year level Coordinator and IT Manager as soon as possible.

1.1 Prohibited Activities

Students are not permitted to do any of the following with College ICTs:

- install, copy, or delete software
- remotely control or message any other computer
- change computer system settings or attempt to bypass network security procedures or settings in any way whatsoever (e.g. proxy servers)
- play games unless under the direction and supervision of a staff member
- download or stream audio or video content without the staff member's permission
- use peer-to-peer file sharing software
- use an external network while at College (e.g. tethering or using hotspots to mobile devices) using a personal laptop, mobile phone or any other portable networking device.
- use student email accounts for anything other than academic purposes
- log on to another student's profile or use another student's account.

1.2 Data Storage and Retrieval

Instructions on the storage of College-related data will be given at the beginning of the school year, however it remains the responsibility of the student to save and back up their work. Loss of data will not be accepted as an excuse for late, or non-submission of work. All College-related data should be saved and backed up on the College network, in cloud storage and on a removable storage device (external hard drive, USB, etc.)

To assist the security of stared data, students must:

- immediately report any interference to their personal files or email
- ensure device is sufficiently charged (above 80% charged as a minimum) before bringing the device to College to prevent disruption in learning or unnecessary safety hazards (i.e. trip hazard from

charging cords across classroom floors)

- not store personal files on any College device or the College-issued cloud storage without permission from a staff member
- not attempt to access files that belong to another student or staff member
- never use their own ICT devices (phones, MP3 players, cameras, etc.) or for data storage at College.

1.3 Security and Cyber-safety

Students will be instructed as part of their education about security and cyber-safety. Passwords will expire and need to be updated on a regular basis. Students should never log on to the network with anyone else's username and password, or let anyone else know their password. Students must immediately report any suspicious activity to a teacher regardless of how harmless it may seem.

A student must not, without permission from a staff member:

- reveal their personal information on the Internet
- go to any site that is not related to College work for educational purposes
- go to gaming sites
- go to chat rooms or use any social networking sites or personal blogs at College.

Additionally, a student must never:

- click on any advertising material
- send email, or view or share internet material that is offensive, or contains content against the Christian values of the College
- distribute or publish any media stored on the College's server (e.g. copying a photo from the media drive and posting on social media). All media remains the property of the College.

Any breach of these conditions will result in College discipline. See *HCC Behaviour Management Policy.*

2. Use of own ICTs

2.1 Mobile phones

Mobile phones may be required for a student to contact a parent after school, however, they are not to be used during the College hours in any form, and must be completely switched off. All phones should be left in a student's locker or bag, or at the College Office and collected at the end of the day. Any phone seen during College hours or activities by a staff member, may be confiscated for the day. Repeated breaches of College rules will be dealt will according to the *HCC Behaviour Management Policy.*

The College has mobile phones and landlines as well as other means of contact that can be used in an emergency.

2.2 Smartwatches

Students should not wear their smartwatch to College or College activities. However, if the smartwatch is being used as a timepiece only (i.e. in *flight mode*), it will be allowed, so long as the student does not breach any of the conditions contained in the *HCC Student Smartwatch Use Policy*.

2.3 Other Internet Connective Technology

Unless, specifically given permission for a special event at College, or for learning impairment issues, other technology must not be brought to College due to both safety concerns and the possibility that the item will be lost or damaged at College.

3. Use of social media and internet

The use of social media and other forms of electronic communication (including posting on forums, sending emails, messaging and texting, etc.) must always be done in safe and respectful manner. Access to the internet at College should only be for educational purposes.

Students are not to access to social media during the course of the College timetable. In their own time students should be aware of:

- their legal responsibilities regarding comments or images being placed on such networks (e.g. disrespectful comments, harassment, bullying, ‘sexting’, etc.)
- their *digital footprint* and the long-term consequences of inappropriate social networking on their personal lives, and future employment opportunities
- students are not to post images to any online medium which identify the College, themselves or any other student in College uniform
- safe practices when using social media.

4.1 Inappropriate Use

A student must not use social media or electronic communication to:

- waste lesson time that is meant for learning or study
- communicate with people at or outside of the College during the College timetable hours
- damage the reputation of the College or any member of its community
- refer to the College or any member of its community to promote ideas that are not in keeping with the College’s values
- share images or material without correct permissions, or of an inappropriate nature, that may damage the College reputation or its members.
- share views while pretending to be another person
- break any of the all College rules.

Other relevant policies and documents:

- HCC Behavioural Management Policy
- HCC Mobile Phone Use Policies
- HCC Privacy Policy
- HCC Recording & Image Use Policy
- HCC Smartwatch Policy
- HCC Social Media Use Policies
- Staff Manual (current edition)

Version history

Previous versions superseded: July 2018, August 2019, October 2021

Review

The policy will be reviewed every two years. Reviews will be conducted with feedback from staff and leadership of the College, and the *Association of Independent Schools of South Australia (AISSA)* who will advise on external changes, such as changes to legislation, good practice, etc.